REMARKS

This Amendment is in response to the Office Action dated January 30, 2008 ("OA"). In the Office Action, claims 30-38 were rejected under 35 USC §101 and claims 30-38 were rejected under 35 USC §103. By this Amendment, claim 30 is amended. Claims 30-38 are believed allowable, with claim 30 being an independent claim.

CLAIM REJECTIONS UNDER 35 USC §101:

Claim 30

Claim 30 is rejected under 35 USC §101 as allegedly directed to non-statutory subject matter. OA, pg. 2. In rejecting claim 30, the Examiner alleges, "Claims 30-38 relate to a system however this system fails to positively recite any actual hardware to constitute a system." *Id.* The Examiner further alleges, "The claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the mean of 35 USC §101." *Id.*

By this Amendment, claim 30 is amended to recite, "a first system comprising a processor." Those skilled in the art will appreciate that a processor is a physical article. More specifically, a processor is hardware. Because claim 30 recites a structure which constitutes a physical article, the system of claim 30 constitutes a machine and/or a manufacture within the meaning of 35 USC §101. Therefore, the Applicants respectfully submit that claim 30 recites statutory subject matter.

For at least these reasons, claim 30 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 30.

Claims 31-38

Claims 31-38 are dependent on and further limit claim 30. Since claim 30 is believed allowable, claims 31-38 are also believed allowable for at least the same reasons as claim 30.

CLAIM REJECTIONS UNDER 35 USC §103:

Claims 30-36 and 38 are rejected under 35 USC §103(a) as unpatentable over U.S. Patent No. 6,834,350 issued to Boroughs et al. ("Boroughs") in view of U.S. Patent No. 6,971,026 issued to Fujiyama et al. ("Fujiyama"). OA, pg. 3.

Claim 37 is rejected under 35 USC §103(a) as unpatentable over Boroughs in view of Fujiyama and further in view of U.S. Patent No. 6,990,591 issued to Pearson ("Pearson"). OA, pg. 6.

A *prima facie* case for obviousness can only be made if the combined reference documents teach or suggest all the claim limitations. MPEP 2143. Additionally, to establish a *prima facie* case of obviousness, there must be some clear articulation of the reason(s) why the claimed invention would have been obvious. *Id.*

Claim 30

Claim 30 recites, in part, "a first system comprising a processor, the first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information." Thus, claim 30 requires reviewing security and vulnerability information from information publishers. Claim 30 further requires that the activation token is provided based on the security and vulnerability information which was reviewed.

The Examiner alleges that column 2, line 59 through column 3, line 10 of Boroughs teaches "a first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information." OA, pg. 3. The cited passage recites:

> Distributions are preferably prepared by a team of network security experts. A distribution may contain information, such as textual information, for review by a network security administrator. For example, the distribution could contain information describing a newly-discovered form of network attack, and explain how network security equipment or software already being used by the subscriber protects the subscriber from such attacks. A distribution may also contain software. Such software can include both software designed to execute once to ensure that the subscriber's network is protected from a certain type of attack, or new or updated network security software that executes continuously to ensure the security of the subscriber's network. A distribution may also contain data used for network security purposes. For example, where a subscriber uses a particular network security device that operates based upon a set of security rules, a distribution to the subscriber may contain additional rules to be added to the set used by the network security device. Boroughs, col. 2, ln. 59 through col. 3, ln. 10.

Thus, Boroughs discloses that a team of network security experts prepares distributions. However, the cited passage fails to teach or suggest

that the network security experts review security and vulnerability information. Nor does the cited passage teach or suggest that the distributions are provided based on security and vulnerability information which was reviewed. Additionally, there is no disclosure in Boroughs that the team of network security experts includes a processor. Therefore, the team of network security experts and the method steps performed thereby fail to teach or suggest the first system of claim 30.

More generally, the passage cited by the Examiner fails to recite any specific steps performed by the team of network security experts to prepare the distributions. Therefore, the cited passage fails to provide sufficient information to enable one of ordinary skill in the art to reconstruct the operations by which the distributions are prepared. Because the cited passage fails to provide an enabling disclosure of preparing the distributions, the preparation of the distributions cannot teach the first system of claim 30.

Furthermore, it *may* be possible for a team of network security experts to discover a vulnerability through original security research. It *may* also be possible for the team to prepare a distribution addressing the vulnerability based on the original security research. However, the resulting distribution would not be provided based on reviewed security and vulnerability information. It follows that a distribution is not provided based on reviewed security and vulnerability information. However, claim 30 requires that the activation token is provided based on reviewed security and vulnerability information. Therefore, a distribution is clearly not equivalent to the activation token recited by claim 30.

Moreover, the network security administrator disclosed by Boroughs clearly does not receive the distribution until after the distribution is prepared. Actions on which preparing a distribution as disclosed by Boroughs is based must occur before the distribution is prepared. Therefore, it is impossible for the distribution to be provided based on any action taken by the network security administrator. Thus, even though Boroughs suggests that the network security administrator reviews distributions, such a review by the network security administrator cannot teach or suggest providing an activation token based on reviewed security and vulnerability information as required by claim 30.

The remainder of the passage cited by the Examiner discloses content which a distribution may contain. Such content includes “information”,

"software" and "data". Information and data are clearly not equivalent to a first system configured to at least review security and vulnerability information from information publishers and to provide the activation token based on the security and vulnerability information. Moreover, Boroughs does not disclose that the software is configured to review security and vulnerability information. Nor does Boroughs disclose that the software is configured to provide an activation token based on the security and vulnerability information. It follows that the software disclosed by Boroughs is not equivalent to the first system of claim 30. Therefore, the Applicants respectfully submit that the cited passage clearly fails to teach or suggest the first system of claim 30.

Claim 30 further recites, in part,

> a second system configured to determine whether the activation token is relevant by checking if actual characteristics at the second system correspond to the system characteristics identified by the activation token, the second system further configured to transform the activation token into at least one activation measure if the activation token is considered relevant by the second system, the activation measure configured to modify services executing at the second system.

Thus, claim 30 requires a second system configured to determine whether the activation token is relevant. Moreover, it is evident from antecedent basis that this second system is the same second system at which the activation measure is configured to modify executing services. Therefore, Boroughs cannot teach claim 30 unless the activation measure is configured to modify services executing at the same system which is configured to determine whether the activation token is relevant.

The Examiner alleges that column 3, lines 35-67 and column 4, lines 1-5 of Boroughs teach the limitation of claim 30 cited above. OA, pg. 3-4. The cited passage recites,

> After the distribution is addressed to addressees among the registered subscribers, the facility attempts to deliver the distribution to each of the addressees to which the distribution is addressed. The facility may preferably deliver distributions either by secure email sent from the network security information service to the addressees, or using a client polling procedure in which a client program at each subscriber periodically polls a server maintained by the network security information service for new distributions addressed to its subscriber. In order to implement the client polling procedure, in certain embodiments, the facility utilizes BackWeb Foundation software, available from BackWeb Technologies of San Jose, Calif. For emailed distributions, a verified email address for the subscriber is

> preferably used. For distributions delivered by the client polling procedure, polling requests from the client preferably include a secret unique identifier issued to the subscriber, encrypted using public key encryption. These measures help ensure that the distribution is delivered only to the subscribers to which it is addressed.
>
> During delivery, each distribution is preferably encrypted to prevent anyone intercepting the distribution from discerning its content. Each distribution is preferably also signed in way that reliably indicates both (1) the source of the distribution, and (2) the contents of the distribution when the distribution left its source. This signature is preferably used by a component of the facility executing at each subscriber to ascertain whether each distribution (1) is from the network security information service or another trusted source and (2) has not been altered since it left that source. The subscriber component of the facility preferably only allows the subscriber to make use of distributions meeting both of these conditions.
>
> The client program of the facility preferably also alerts a user at the subscriber as soon as a distribution is received, displays information about the distribution, and facilitates the application of the distribution to enhance the level of security of the subscriber's network. Boroughs, col. 3, ln. 35 through col. 4, ln. 5.

In a passage preceding the above passage, Boroughs states, "The present invention provides a software facility for the secure and differentiated delivery of network security information ('the facility') to support a network security information service." Boroughs, col. 2, ln. 48-51. Thus, it is evident that "the facility", as the term is used by Boroughs, is a software facility for the delivery of network security information.

The final sentence of the passage cited by the Examiner teaches that the facility facilitates the application of the distribution to enhance the level of security of the subscriber's network. The facility is clearly not equivalent to the subscriber's network. It follows that the facility is not equivalent to the system to which the distribution is applied.

As previously noted, claim 30 requires a second system configured to determine whether the activation token is relevant. The Applicants respectfully submit that the passage cited by the Examiner is devoid of any discussion of determining whether the activation token is relevant. Therefore, the passage cited by the Examiner cannot, by itself, teach the second system of claim 30.

The paragraph immediately preceding the passage cited by the Examiner recites,

> Because some distributions are only useful to subscribers having certain security characteristics, such as those having a particular network security device, the facility preferably selects addressees for each distribution from the subscribers registered with the network security information service. In this regard, the facility preferably uses a subscriber information database that stores information about each subscriber registered with the network security information service. For example, the subscriber database may contain, for each subscriber, an indication of the types of network security equipment, network security software, and applications used by the subscriber. When the facility receives a new distribution, it preferably receives with it an addressing query designed to select addressees for the distribution. The facility performs the addressing query against the subscriber information database to select addressees of the distribution. By selecting addressees for a distribution (or "addressing" the distribution), the facility maximizes the extent to which each registered subscriber receives the distributions that relate to it, and minimizes the extent to which each registered subscriber receives distributions that do not relate to it. Also, by directly controlling the set of addressees, the facility ensures that distributions are not delivered to parties other than subscribers. Boroughs, col. 3, ln. 11-34.

This passage discloses that the facility performs the addressing query against the subscriber information database to select addressees of the distribution. However, as previously noted, the facility is not equivalent to the system to which the distribution is applied. Moreover, as previously noted, claim 30 requires that the activation measure is configured to modify services executing at the same system which is configured to determine whether the activation token is relevant. Therefore, even assuming *arguendo* that the distribution is equivalent to an activation token, that the steps performed by the facility are equivalent to determining whether the distribution is relevant, and that the distribution is configured to modify services executing at the system to which it is applied, the facility nonetheless fails to teach the second system of claim 30. This is evident because even in this case, the facility would not modify services executing at itself.

Moreover, Figure 17 of Boroughs discloses a flowchart of steps performed by the subscriber. Figure 17 shows that if a distribution is received at step 1706, the distribution is always processed. The only possible exception is if the security check at step 1710 finds that one-way function results failed to match. However, this is an exception condition which should only occur if the distribution is corrupt or unauthorized. Specifically, the security check at step 1710 is clearly not equivalent to a

determination whether the distribution is relevant. Thus, Figure 17 teaches that the system to which the distribution is being applied does not make a determination whether the distribution is relevant. This teaches away from an activation measure configured to modify services executing at the same system which is configured to determine whether the activation token is relevant as required by claim 30.

The Examiner further states, "wherein the first system is further configured to automatically filter the security and vulnerability information relevant to the system characteristics identified by the activation token (see column 2 line 59 through column 3 line 10 and Figure 17)." OA, pg. 4.

The Applicants respectfully submit that claim 30 does not recite the limitation cited above by the Examiner. The limitation cited above is recited in claim 33. Thus, the question of whether Boroughs teaches the cited claim limitation is not relevant to the question of whether claim 30 is allowable.

The Examiner further argues that ". . . it would have been obvious to a person of ordinary skill in the art to include trust levels with the activation tokens of Boroughs et al. Motivation to do so would have been to distinguish between the types of threats (see figures 2-5 and column 7 line 54 through column 8 line 55)." OA, pg. 4.

The Applicants respectfully submit that neither claim 30 nor Fujiyama recites "trust levels". Instead, Fujiyama shows a "security level" in Figures 2-5. Nonetheless, Boroughs fails to express any appreciation of the benefits of distinguishing between different types or levels of security threats. To the contrary, as discussed above, Figure 17 of Boroughs teaches that the system receiving a distribution always processes the distribution unless the distribution fails a security check. This teaches away from a system which processes distributions selectively based on the type or level of threat which the distribution concerns. For this reason, one would not be motivated to reconstruct Boroughs in light of Fujiyama to create a system which includes the security levels disclosed by Fujiyama in activation tokens in order to distinguish between different types of threats.

For at least these reasons, claim 30 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 30.

Claim 31

Claim 31 is dependent on and further limits claim 30. Since claim 30 is believed allowable, claim 31 is also believed allowable for at least the same reasons as claim 30.

Claim 32

Claim 32 recites, "The system of claim 30, further comprising a reporting means configured to report to a system administrator of the second system any activation measures taken by the second system." Thus, claim 32 requires not only a report to a system administrator but additionally requires that the report comprises any activation measures taken by the second system.

Moreover, claim 30 recites, "the second system further configured to transform the activation token into at least one activation measure." Thus, an activation measure, as the term is used in claim 32, is clearly required to be a result of a transformation of an activation token.

The Examiner alleges that "the modified Boroughs et al. and Fujiyama et al. system" teaches the limitation introduced by claim 32. OA, pg. 4. In support of this position, the Examiner cites column 2, lines 59-67 of Boroughs. *Id.* The passage cited by the Examiner states,

> Distributions are preferably prepared by a team of network security experts. A distribution may contain information, such as textual information, for review by a network security administrator. For example, the distribution could contain information describing a newly-discovered form of network attack, and explain how network security equipment or software already being used by the subscriber protects the subscriber from such attacks. A distribution may also contain software. Such software can . . . . Boroughs, col. 2, ln. 59-67.

The cited passage of Boroughs discloses information being reviewed by a network security administrator. The passage discloses that a distribution may contain information for review by a network security administrator. However, the Examiner has not explained, and it is not apparent, how such information is equivalent to activation measures taken by the second system. The passage further discloses that the information may be "textual information" or "information describing a newly-discovered form of network attack." However, neither of these types of information is equivalent to a report to a system administrator of activation measures.

The passage additionally discloses that a distribution may contain "software." Furthermore, immediately following the cited passage at column 3, line 5, Boroughs discloses that the distribution may contain "data." However, neither software nor data is equivalent to a report to a system administrator of activation measures.

The cited passage further outlines an example wherein the distribution explains "how network security equipment or software already being used by the subscriber protects the subscriber from such attacks." However, as previously noted, claim 32 requires that an activation measure results from the transformation of an activation token. It is apparent from the words, ". . . already being used . . .", that the network security equipment or software was already employed prior to receiving the distribution. It follows that the network security equipment or software is clearly not a result of a transformation of the exemplary distribution. Therefore, even assuming *arguendo* that the exemplary distribution is equivalent to an activation token, the network security equipment or software cannot be equivalent to an activation measure. Accordingly, the Applicants respectfully submit that the example disclosed in the passage cited by the Examiner fails to teach a reporting means configured to report to a system administrator of the second system any activation measures taken by the second system as required by claim 32.

Therefore, the Applicants respectfully submit that the cited passage of Boroughs and the distributions disclosed therein fail to teach or suggest a reporting means configured to report to a system administrator of the second system any activation measures taken by the second system as required by claim 32.

For at least these reasons, claim 32 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 32.

Claim 33

Claim 33 is dependent on and further limits claim 30. Since claim 30 is believed allowable, claim 33 is also believed allowable for at least the same reasons as claim 30.

Claim 34

Claim 34 is dependent on claim 30 and recites, "The system of claim 30, further comprising a list of a plurality of trusted service providers from whom activation tokens are accepted by the second system."

The Examiner alleges that "the modified Boroughs et al. and Fujiyama et al. system discloses a list of trusted service providers from whom activation tokens are accepted by the second system." OA, pg. 5. In support of this position, the Examiner cites column 8, lines 13-39 of Fujiyama. *Id.*

It is well settled that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336, quoted with approval in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007).

In rejecting claim 34, the Examiner alleges that Fujiyama discloses "a list of trusted service providers from whom activation tokens are accepted by the second system." OA, pg. 5. The Examiner argues that this structure is found in Fujiyama by merely citing the text quoted above and citing Fujiyama column and line numbers in parentheses. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 34 disclosed in Fujiyama. If the rejection of claim 34 is maintained, the Applicants request that a detailed explanation of disclosed structures relied upon in Fujiyama be clearly articulated by the Examiner in accordance with 37 CFR 1.104(c)(2).

Furthermore, the passage cited by the Examiner states,

> Also, column 206_i is provided for each of the constituent components, which are intended for use as a component of an objective system. In the case where a security countermeasure described in the box of the security countermeasure in the same row is available to be applied, in the column 206_i there are described a security level L1, L2, or L3 ensured by applying the security countermeasure, an annual required cost C1, C2, C3, C4, or C5 necessary to apply the security countermeasure, and a remaining risk R1, R2, R3, R4, or R5 shown by annual damages arising when the assumed threat described in the box of

> an assumed threat in the same row is turned into reality by not applying the security countermeasure.
>
> Further, column 207 is provided for a facility in which constituent components intended for use as the components of an objective system are installed. In the case where the security countermeasure described in the box of the security countermeasure in the same row is available to be applied, as is the case with the column 206_i, in column 207 are described a security level L1, L2, or L3 ensured by applying the security countermeasure, an annual requirement cost C1, C2, C3, C4, or C5 necessary to apply the security countermeasure, and a remaining risk R1, R2, R3, R4, or R5 shown by annual damages arising when the assumed threat described in the box of the assumed threat in the same row is turned into reality by not applying the security countermeasure. Fujiyama, col. 8, ln. 13-39.

The Applicants respectfully submit that the cited passage of Fujiyama fails to teach or suggest a list of a plurality of trusted service providers from whom activation tokens are accepted by the second system as required by claim 34.

For at least these reasons, claim 34 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 34.

Claim 35

Claim 35 is dependent on claim 30 and recites, "The system of claim 30, wherein the at least one preset activation measure is shutting down a service affected by the specified threat level."

In rejecting claim 35, the Examiner alleges that "the modified Boroughs et al. and Fujiyama et al. system discloses a preset activation measure is one of shutting down a service affected by the specified threat level and reconfiguration of the service." OA, pg. 5. In support of this position, the Examiner cites Figure 3, column 202 of Fujiyama. *Id.*

Figure 3, column 202 of Fujiyama is a column in a table titled, "Security Countermeasure." One of the cells under this column contains the text, "Stop an Unnecessary Service." *Id.*

Fujiyama states, "In the case where a security countermeasure described in the box of the security countermeasure in the same row is available to be applied, in the column 206_i there are [sic] described a security level L1, L2, or L3 ensured by applying the security countermeasure . . . ." Fujiyama, col. 8, ln. 15-19. It is thus evident that a security level is a level of security ensured by applying the security countermeasure.

Moreover, Figures 2-5 of Fujiyama contain the legend, "Security Level: L1: Normal, L2: Strong, L3: Strongest." Thus, Fujiyama discloses security levels which are defined in terms of a quantity of security provided by each level.

It follows that a security level, as the term is used by Fujiyama, is a quantity or level of security. A quantity or level of security does not affect a service. Therefore, the Applicants respectfully submit that even assuming *arguendo* that the security level taught by Fujiyama is equivalent to a threat level, Fujiyama fails to teach or suggest shutting down a service affected by the specified threat level as required by claim 35.

Moreover, the Applicants respectfully submit that none of the remaining security countermeasures depicted in Figure 3, column 202 of Fujiyama are equivalent to shutting down a service. Therefore, none of the remaining security countermeasures depicted in Figure 3, column 202 of Fujiyama teach or suggest shutting down a service affected by the specified threat level as required by claim 35.

For at least these reasons, claim 35 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 35.

Claim 36

Claim 36 is dependent on claim 30 and recites, "The system of claim 30, wherein the at least one preset activation measure is reconfiguring the functionality of a service affected by the specified threat level."

In rejecting claim 36, the Examiner alleges the same rationale as for claim 35. OA, pg. 5.

The Applicants respectfully submit that for the reasons discussed above in regards to claim 35, a security level, as the term is used by Fujiyama, is a quantity or level of security. A quantity or level of security does not affect a service. Therefore, the Applicants respectfully submit that even assuming *arguendo* that a security level taught by Fujiyama is equivalent to a threat level, Fujiyama fails to teach or suggest reconfiguring the functionality of a service affected by the specified threat level as required by claim 36.

For at least these reasons, claim 36 is believed allowable. The Applicants respectfully request reconsideration and allowance of claim 36.

Claims 37 and 38

Claims 37 and 38 are dependent on and further limit claim 30. Since claim 30 is believed allowable, claims 37 and 38 are also believed allowable for at least the same reasons as claim 30.

CONCLUSION

In view of the forgoing remarks, it is respectfully submitted that this case is now in condition for allowance and such action is respectfully requested. If any points remain at issue that the Examiner feels could best be resolved by a telephone interview, the Examiner is urged to contact the attorney below.

No fee is believed due with this Amendment, however, should such a fee be required please charge Deposit Account 50-0510 the required fee. Should any extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: April 30, 2008

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (866) 607-8538